UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville Division

In the Matter of the Search of)
)
Dell Laptop Computer)
Model Number P62G)
Serial Number 8DP9RC2)

Case No. 5:19-CM-63

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe property to be searched and give its location)*: ***SEE ATTACHMENT "A". This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A) and Federal Rule of Criminal Procedure 41***

located in the Western District of Arkansas, there is now concealed *(identify the person or describe the property to be seized)*:
SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ■ evidence of a crime;
- ■ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Possession/Distribution of Child Pornography

The application is based on these facts:

■ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gerald Faulkner, Special Agent HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/17/19

Judge's signature

City and state: Fort Smith, Arkansas

Mark E. Ford, United States Magistrate Judge
Printed name and title

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The following electronic device (**SUBJECT ITEM**) seized by HSI and currently located at the HSI office in Fayetteville, Arkansas, from the Fayetteville, Arkansas Virtual Academy and property of the Fayetteville, Arkansas Public School System known to have been possessed and operated by Nathan HENRY:

001 – Dell Laptop Computer, model number P62G bearing the serial number 8DP9RC2

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

a. Any and all images of suspected child pornography and files containing images of suspected child pornography, any and all images believed to be an attempt to produce child pornography, in any form wherever it may be stored or found including, but not limited to:

i. originals, thumbnails, and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. videos (AKA motion pictures, films, film negatives), and other recordings or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. Images self-produced of the defendant and minors, and attempts to take or produce such.

iv. Images of children, nude or otherwise, possessed, sent, received, or via message, email, or otherwise stored on the phone.

v. Internet history, including CACHE memory related to internet searches for child pornography or websites that could pertain such.

b. information or correspondence pertaining to the solicitation of others for sexual activity involving minors, and any and all information, messages, etc related to the sexual exploitation of children, including but not limited to:

i. correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, text messages, establishing possession, identity of individuals, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

ii. records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.

iv. Any and all chat log, text messages, email, or any type of communication in any form that is related to the sexual exploitation of minors for sexual purposes or related to the production, distribution or possession of child pornography.

c. records evidencing ownership of the subject item, including in and all lists of names, telephone numbers, addresses and contacts, and the content of voice mails and text messages and internet based applications, and internet or purchase history for any and all sexual devices, including but not limited to dildos, vibrators and sexual games.

d. Any and all security devices, to include encryption devices, needed to gain access to the devices;

e. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.

f. Any and all recordings, including those made by the defendant or the minor victim, or anyone else that depicts the defendant or others engaging in sexually explicit conduct of any type.

g. In searching the data, the computer personnel may examine and copy all of the data contained in the subject item to view their precise contents and determine whether the data falls within the items to be seized. In addition, the examining personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS :
:
: **ss. AFFIDAVIT**
:
COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, Gerald Faulkner, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since April, 2009. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography offenses. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

2. This affidavit is being submitted in support of an application for a search warrant

for an electronic device described as being a Dell Laptop Computer, model number P62G bearing the serial number 8DP9RC2, also referred to as "**SUBJECT ITEM**" located and seized from the Fayetteville, Arkansas Virtual Academy and property of the Fayetteville, Arkansas Public School System. The **SUBJECT ITEM** is currently being stored at the HSI office in Fayetteville, Arkansas. As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

Statutory Authority

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

a. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person's interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

Computers and Child Pornography

4. Based upon my knowledge and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of

computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-base/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

5. In addition, based upon my own knowledge and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography in these ways.

6. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography

can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

7. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial Internet Service Providers (ISPs), such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

8. The Internet allows users, while still maintaining anonymity, to easily locate other individuals with similar interests in child pornography; and websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography

over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.

9. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously with the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

10. Based on my experience and consultation with computer forensic experts, I know that electronic files can be easily moved from computer or electronic storage medium to another computer or medium. Therefore, electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same or a different location.

11. It should be noted that Internet Protocol (IP) numbers are unique identifiers leased to internet customers by their ISP's. Although IP numbers are capable of changing over time, only one (1) unique IP number can be assigned to a given customer's computer at any given time. Logs of these leased IP's (and their assigned customer accounts) are stored by ISP's routinely.

12. Your Affiant knows from his own experience and the training and experience of other law enforcement officers that Internet computers identify each other by an Internet Protocol

or IP address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that uses the address to access the Internet.

13. Law Enforcement uses specialized "peer to peer" (P2P) software to locate computers offering to participate in the distribution of child pornography images and files over P2P sharing networks in Arkansas. Millions of computer users throughout the world use P2P file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

14. The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

15. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.

16. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading.

17. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".

18. Files or sets of files are shared on the BitTorrent network via the use of "Torrents". A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download.

19. The strength of a Peer to Peer Network is that it bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the fingerprinting of files. Once you check a file with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is called secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

20. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent". This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent"

file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers".

21. "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent". "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publically available servers on the Internet that provide BitTorrent tracker services.

22. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and the piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves.

23. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the

BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent", to include the remote peers/clients Internet Protocol (IP) addresses.

24. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website.

25. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file.

26. Utilizing "trackers" and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files.

27. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file.

28. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external

storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

29. Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents can quickly identify targets in their jurisdiction.

30. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

31. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program

and version being utilized by the suspect computer. The law enforcement has the ability to log this information.

32. It should be noted, during the downloading and installation of the publically available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading. uTorrent accelerates downloads by enabling your computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility.

33. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded.

34. Additionally, your Affiant knows that P2P software may display the Globally Unique Identifier (GUID) identification number of computers offering to share files on the network. A Globally Unique Identifier or GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of

unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your Affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

Summary of Investigation to Date

35. In October 2018, a HSI Internet Crimes Against Children (ICAC) Task Force affiliate was conducting an online investigation on the BitTorrent Peer-to-Peer (P2P) file sharing network for offenders sharing child pornography. During the course of the online investigation, a connection was made between the HSI ICAC Task Force affiliate's investigative computer and a computer/device running BitTorrent software from an IP Address of 72.206.6.202. During the course of the online investigation, on or about October 8, 2018, approximately twenty-four (24) files were downloaded from IP Address 72.206.6.202. The device at IP Address 72.206.6.202 was the only IP Address which shared the contents for the files downloaded, and as such, the files were downloaded directly from this IP Address. While connected to IP Address 72.206.6.202, the HSI ICAC Task Force affiliate's investigative computer, at the time, captured approximately fifty-three (53) files being made available for public sharing within the network containing titles consistent with child pornography such as, "baby_girl", "teen" and "14old". The HSI Task Force affiliate then determined the IP Address was geo-located to Bentonville, Arkansas at which time the lead information and downloads were forwarded to the HSI Assistant Special Agent in Charge Office in Fayetteville, Arkansas for further investigation.

36. In March 2019, while utilizing ICAC investigative software tools, your Affiant initiated a search of the IP Address 72.206.6.202 which revealed the particular IP Address, at that time, was recorded as having approximately ten (10) files of interest consistent with child

exploitation, with one (1) of those files considered to be "severe". The dates and times of the flagged files of interest through the BitTorrent software were ranging from approximately January 11, 2018 to November 5, 2018.

37. In March 2019, your Affiant viewed two (2) of the files successfully downloaded by the HSI ICAC affiliate from IP Address 72.206.6.202. Your Affiant more particularly described the files as follows:

(a) File Name: **2crazy14oldchickz1.mp4**

This video is approximately thirty-two (32) minutes in length and depicts two minor females approximately thirteen (13) to fourteen (14) years of age interacting and performing on what appears to be a live streaming website camera. During the course of the video, the minor females are seen undressing themselves and exposing their breasts, vaginas and anuses to the website camera while interacting with other unknown online users.

(b) File Name: **same14_2GIRLS.wmv**

This video is approximately twenty-two (22) minutes in length and depicts two minor females approximately thirteen (13) to fifteen (15) years of age interacting and performing on what appears to be a live streaming website camera. During the course of the video, the minor females are seen undressing themselves, self-masturbating and also exposing their breasts, vaginas and anuses to the website camera while interacting with other unknown online users.

38. An internet search on the origin of the IP Address 72.206.6.202 found it to be issued to the internet service provider Cox Communications. A federal summons was issued to Cox Communications in reference to IP Address 72.206.6.202 for the specific date and time the two (2) previously described videos of child pornography were successfully downloaded from the user. Documents received on or about November 14, 2018 from Cox Communications identified the IP Address as being assigned to Nathan HENRY at 503 Cherry Street in Pea Ridge, Arkansas, as an active account with a date of service going back to March 24, 2017.

39. Your Affiant conducted Department of Homeland Security (DHS) database queries on Nathan HENRY and the residence. Nathan HENRY is believed to have been born in 1977 and issued the Social Security Administration number ending in the last four digits 7133. HENRY is issued an Arkansas Driver's License ending in the last four numbers 7555 which was issued in 2018 and expires in 2026. The address associated to the Arkansas Driver's License is listed as being 503 Cherry Street in Pea Ridge, Arkansas 72751.

40. On April 30, 2019, your Affiant contacted Officers from the Pea Ridge, Arkansas Police Department and requested any and all current utility records for the residence located at 503 Cherry Street in Pea Ridge, Arkansas 72751. On May 1, 2019, your Affiant was notified by Officers that active water services were being paid through HENRY from approximately March 21, 2017 to the present at 503 Cherry Street in Pea Ridge, Arkansas 72751.

41. On May 9, 2019, pursuant to the ongoing child exploitation investigation, HSI Special Agents and Task Force Officers (TFO) assigned to the ICAC Task Force, along with Officers from the Pea Ridge, Arkansas Police Department and Bentonville, Arkansas Police Department, arrived at the residence of HENRY located at 503 Cherry Street in Pea Ridge, Arkansas to execute a federal search warrant for possible violations of Title 18, United States Code, Section 2252A – Possession/Distribution of Child Pornography.

42. During a post-Miranda interview, your Affiant questioned HENRY about what electronic devices were located within the residence. He replied there was one desktop computer, one laptop, his daughter's Chromebook that was issued by her school, two iPads, three iPhones and approximately four other cellular telephones located in the house. HENRY stated he also has a school issued laptop that he does not bring home and was currently at the Fayetteville, Arkansas Virtual Academy where he works as a teacher.

43. Following the execution of the federal search warrant at HENRY's residence, your Affiant made contact with an administrator from the Fayetteville, Arkansas Virtual Academy and informed them there was an ongoing case involving HENRY. Based on the investigation, your Affiant advised the administrator HENRY's school issued laptop was going to be seized by HSI. The administrator confirmed the laptop was in HENRY's office, where Henry works part of the time, and the device was retained until your Affiant arrived at the school and took custody of the computer. Your affiant is aware that **SUBJECT ITEM** is property of the Fayetteville Arkansas School System, and that as such Henry does not have a right to privacy of the device; however, a search warrant is being sought in an abundance of caution.

44. Your Affiant respectfully requests a federal search warrant be issued for the Dell Laptop Computer, model number P62G bearing the serial number 8DP9RC2 (**SUBJECT ITEM**) located and seized by HSI from the Fayetteville, Arkansas Virtual Academy and property of the Fayetteville, Arkansas Public School System. This federal search warrant is being sought to allow HSI ICAC CFAs the opportunity to conduct in-depth forensic examinations on the device, known to have been possessed and operated by HENRY, to ensure he has not utilized his school issued laptop to view files or download software programs related to image/videos containing child pornography.

Conclusion

45. *Necessity of On-site and Off-site examinations of entire computers or storage media*. Based on my experience and the training and experience of other agents, many of the items sought in this affidavit may be stored electronically. In addition, based on my experience, I know that searching computerized information for evidence of crime often requires special agents to seize most or all of a computer system's central processing unit (CPU), input/output peripheral

devices, related software, documentation, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

(a) Volume of evidence: Computer storage devices such as hard disks, diskettes, tapes and laser disks, can store the equivalent of thousands of pages of information. This sorting process can take up to several months to complete, depending on the volume of data stored. Therefore, it would also be impractical to attempt this type of data search on site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

46. Therefore, authorization is sought in this application to seize the items set forth in attachment "B" that are found on the premises to be searched, in order to examine those items for evidence. If it is determined that data has been seized that does not constitute evidence of the crimes detailed herein, the government will return said data within a reasonable time.

47. Based on my experience and the training and experience of other agents involved with this investigation, your affiant knows that individuals involved in the sexual exploitation of

children through child pornography almost always keep copies of their sexual explicit material. Among the reasons copies are maintained is because child pornography is illegal to openly purchase, and the most common method of acquiring it is by trading with other people with similar interests. It is also known that due to the inherent illegality of these sexually explicit materials, they are most often kept in a place considered secure, usually a residence, to avoid detection by law enforcement.

48. Based on the foregoing information, probable cause exists to believe there is located on the Dell Laptop Computer, model number P62G bearing the serial number 8DP9RC2, the **SUBJECT ITEM**, evidence of violations of Title 18, United States Code, Section 2252, et seq. Your Affiant prays upon his honorable court to issue a search warrant for the **SUBJECT ITEM** for the items set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2252, et seq.

Gerald Faulkner, Special Agent
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 17 day of May 2019

Mark E. Ford
United States Magistrate Judge